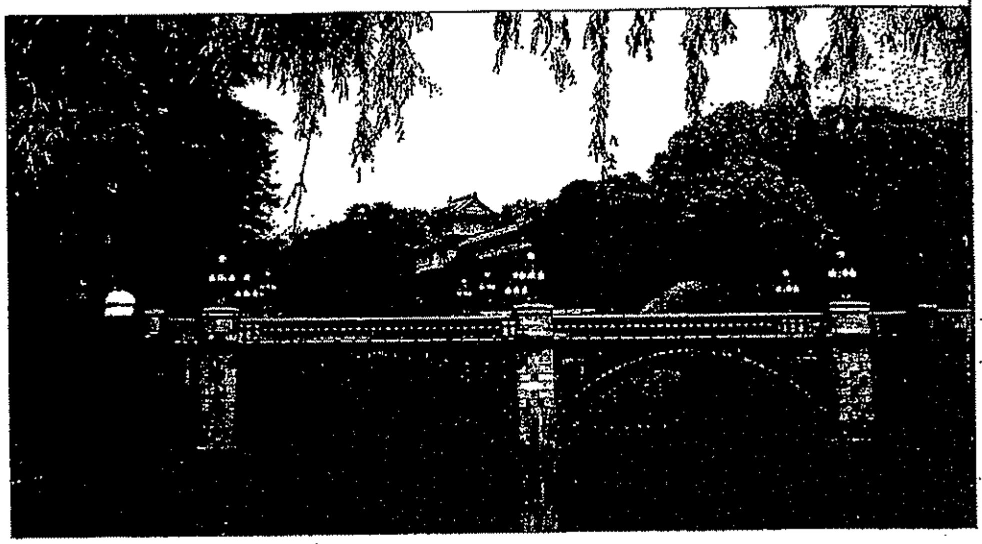
Z

New Riders



Technology Series

Intrusion Detection

Rebecca Gurley Bace

INTRUSION DETECTION

Rebecca Gurley Bace

MTP
MACMILLAN TECHNICAL PUBLISHING U·S·A

Intrusion Detection

Rebecca Gurley Bace

Published by:
Macmillan Technical Publishing
201 West 103rd Street
Indianapolis, IN 46290 USA

International Standard Book Number: 1-57870-185-6

Library of Congress Catalog Card Number: 99-63273

03 02 01 00 7 6 5 4 3 2

Interpretation of the printing code: The rightmost double-digit number is the year of the book's printing; the rightmost single-digit number is the number of the book's printing. For example, the printing code 00-1 shows that the first printing of the book occurred in 2000.

Composed in Galliard and MCPdigital by Macmillan Technical Publishing

Printed in the United States of America

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Macmillan Technical Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

This book is designed to provide information about intrusion detection. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an as-is basis. The authors and Macmillan Technical Publishing shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from th information contained in this book or from the use of the discs or programs that may accompany it.

Feedback Information

At Macmillan Technical Publishing, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us at networktech@mcp.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher
David Dwyer

Executive Editor
Linda Ratts Engelman

Managing Editor
Gina Brown

Product Marketing Manager
Stephanie Layton

Acquisitions Editor
Karen Wachs

Development Editor
Katherine Pendergast

Project Editor
Alissa Cayton

Copy Editor
June Waldman

Indexer
Larry Sweazy

Acquisitions Coordinator
Jennifer Garrett

Manufacturing Coordinator
Chris Moos

Book Designer
Louisa Klucznik

Cover Designer
Aren Howell

Compositors
Scan Communications Group, Inc.
Amy Parker

OVERVIEW

Introduction 1

1 The History of Intrusion Detection 7

2 Concepts and Definitions 27

3 Information Sources 45

4 Analysis Schemes 79

5 Responses 121

6 Vulnerability Analysis: A Special Case 135

7 Technical Issues 155

8 Understanding the Real-World Challenge 173

9 Legal Issues 195

10 For Users 217

11 For Strategists 235

12 For Designers 255

13 Future Needs 275

Appendix A Glossary 289

Appendix B Bibliography 297

Appendix C Resources 315

Appendix D Checklist 321

Index 323

CONTENTS

Introduction 1
Defining Intrusion Detection 3
By Way of Introduction 4
1 The History of Intrusion Detection 7
1.1 Audit: Setting the Stage for Intrusion Detection 7
1.1.1 Differences between Financial and Security Audit 9
1.1.2 Audit as a Management Tool 9
1.1.3 EDP Audits and Early Computer Security 10
1.1.4 Audit and Military Models of Computer Security 11
1.2 The Birth of Intrusion Detection 12
1.2.1 Anderson and the Audit Reduction Problem 12
1.2.2 Denning, Neumann, and IDES 14
1.2.3 A Flurry of Systems through the 1980s 15
1.2.4 Integrating Host and Network-Based Intrusion Detection 21
1.2.5 The Advent of Commercial Products 23
1.3 Conclusion 24
Endnotes 25
2 Concepts and Definitions 27
2.1 An Introduction to Intrusion Detection 27
2.2 Security Concepts 28
2.2.1 A Cultural View of Computer and Network Security 28
2.2.2 Practical Definition of Computer Security 29
2.2.3 Formal Definition of Computer Security 29
2.2.4 Trust 30
2.2.5 Threat 30
2.2.6 Vulnerability 31
2.2.7 Security Policy 32
2.2.8 Other Elements of the System Security Infrastructure 33
2.2.9 How Security Problems Occur 35
2.3 Intrusion Detection Concepts 37
2.3.1 Architecture 37
2.3.2 Monitoring Strategy 38
2.3.3 Analysis Type 38
2.3.4 Timing 40
2.3.5 Goals of Detection 40
2.3.6 Control Issues 42

2.3.7 Determining Strategies for Intrusion Detection 43

2.4 Conclusion 43

Endnotes 44

3 Information Sources 45

3.1 The Organization of this Chapter 45
3.1.1 Which Source Is the Right Source? 46
3.1.2 Enduring Questions 46

3.2 Host-Based Information Sources 47
3.2.1 Operating System Audit Trails 47
3.2.2 Approaches to Structuring Audit Trails 48
3.2.3 Problems with Commercial Audit Systems 48
3.2.4 Pros and Cons of Operating System Audit Trails 49
3.2.5 Content of Audit Trails 49
3.2.6 Audit Reduction 57
3.2.7 System Logs 58
3.2.8 Applications Information 60
3.2.9 Target-Based Monitoring 65

3.3 Network-Based Information Sources 67
3.3.1 Why Network Sources? 67
3.3.2 Network Packets 67
3.3.3 TCP/IP Networks 68
3.3.4 Packet Capture 70
3.3.5 Network Devices 73
3.3.6 Out-of-Band Information Sources 73

3.4 Information from Other Security Products 74
3.4.1 An Example of a Security Product Data Source 74
3.4.2 Organization of Information Prior to Analysis 75
3.4.3 Other System Components as Data Sources 76

3.5 Conclusion 76

Endnotes 77

4 Analysis Schemes 79

4.1 Thinking About Intrusions 79
4.1.1 Defining Analysis 79
4.1.2 Goals 80
4.1.3 Supporting Goals 81
4.1.4 Detecting Intrusions 82

4.2 A Model for Intrusion Analysis 83
4.2.1 Constructing the Analyzer 84

4.2.2 Performing Analysis 88
4.2.3 Feedback and Refinement 89

4.3 Techniques *91*
4.3.1 Misuse Detection 91
4.3.2 Anomaly Detection 100
4.3.3 Alternative Detection Schemes 110

4.4 Conclusion *117*

Endnotes *117*

5 Responses *121*

5.1 Requirements for Responses *121*
5.1.1 Operational Environment 123
5.1.2 System Purpose and Priorities 123
5.1.3 Regulatory or Statutory Requirements 124
5.1.4 Conveying Expertise to Users 124

5.2 Types of Responses *125*
5.2.1 Active Responses 125
5.2.2 Passive Responses 128

5.3 Covering Tracks During Investigation *130*
5.3.1 Fail-Safe Considerations for Response Components 130
5.3.2 Handling False Alarms 130
5.3.3 Archive and Report 131

5.4 Mapping Responses to Policy *131*
5.4.1 Immediate 132
5.4.2 Timely 132
5.4.3 Long-Term—Local 132
5.4.4 Long-Term—Global 133

5.5 Conclusion *133*

Endnotes *134*

6 Vulnerability Analysis: A Special Case *135*

6.1 Vulnerability Analysis *136*
6.1.1 Rationale for Vulnerability Analysis 136
6.1.2 COPS—An Example of Vulnerability Analysis 136
6.1.3 Issues and Considerations 140

6.2 Credentialed Approaches *140*
6.2.1 Definition of Credentialed Approaches 141
6.2.2 Determining Subjects for Credentialed Approaches 141
6.2.3 Strategy and Optimization of Credentialed Approaches 142

6.3 Noncredentialed Approaches *144*
6.3.1 Definition of Noncredentialed Approaches 144
6.3.2 Methods for Noncredentialed Vulnerability Analysis 144
6.3.3 Testing by Exploit 144
6.3.4 Inference Methods 145
6.3.5 A Historical Note 145
6.3.6 Architecture of SATAN 147
6.3.7 Fail-Safe Features 149
6.3.8 Issues Associated with SATAN 149
6.4 Password-Cracking *150*
6.4.1 Concepts of Operation 150
6.4.2 Password Crackers as Vulnerability Analysis Tools 151
6.5 Strengths and Weaknesses of Vulnerability Analysis *151*
6.5.1 Strengths of Credentialed Analysis Techniques 151
6.5.2 Strenghts of Noncredentialed Analysis Techniques 152
6.5.3 Disadvantages 152
6.6 Conclusion *153*
Endnotes *153*
7 Technical Issues ***155***
7.1 Scalability *155*
7.1.1 Scaling over Time 155
7.1.2 Scaling over Space 156
7.1.3 Case Study—GrIDS 157
7.2 Management *157*
7.2.1 Network Management 158
7.2.2 Sensor Control 159
7.2.3 Investigative Support 159
7.2.4 Performance Loads 160
7.3 Reliability *160*
7.3.1 Reliability of Information Sources 161
7.3.2 Reliability of Analysis Engines 162
7.3.3 Reliability of Response Mechanisms 163
7.3.4 Reliability of Communications Links 164
7.4 Analysis Issues *165*
7.4.1 Training Sets for AI-Based Detectors 165
7.4.2 False Positives/Negatives in Anomaly Detection 165
7.4.3 Trends Analysis 166
7.4.4 Composition of Policies 166

7.5 Interoperability 167
7.5.1 CIDF/CRISIS Effort 169
7.5.2 Audit Trail Standards 169
7.6 Integration 171
7.7 User Interfaces 171
7.8 Conclusion 172
Endnotes 172
8 Understanding the Real-World Challenge 173
8.1 The Roots of Security Problems 173
8.1.1 Problems in Design and Development 174
8.1.2 Problems in Management 178
8.1.3 Problems in Trust 181
8.2 Through a Hacker's Eyes 185
8.2.1 Identifying a Victim 185
8.2.2 Casing the Joint 186
8.2.3 Gaining Access 186
8.2.4 Executing the Attack 187
8.3 Security versus Traditional Engineering 191
8.3.1 Traditional Engineering 191
8.3.2 Security Engineering 191
8.3.3 Rules of Thumb 192
8.4 Rules for Intrusion Detection Systems 192
8.5 Conclusion 194
Endnotes 194
9 Legal Issues 195
9.1 Law for Geeks 196
9.1.1 Legal Systems 197
9.1.2 Legislation 198
9.1.3 Civil Litigation/Tort Law 199
9.1.4 Complications in Applying Law to Cyberspace 201
9.2 Rules of Evidence 203
9.2.1 Types of Evidence 203
9.2.2 Admissibility of Evidence 204
9.2.3 Restrictions and Exceptions 205
9.2.4 Provisions for Handling Evidence 205
9.2.5 Rules of Evidence as Applied to System Logs and Audit Trails 206
9.3 Laws Relating to Monitoring Activity 207
9.3.1 When a System Administrator Monitors a System 207

9.3.2 When Law Enforcement Agents Monitor a System 208
9.3.3 Notification of Monitoring 208
9.4 What Real Cases Have Taught Us 208
9.4.1 The Mitnick Case 209
9.4.2 The Rome Lab Case 212
9.4.3 Lessons Learned 214
9.5 Conclusion 215
Endnotes 216
10 For Users 217
10.1 Determining Your Requirements 217
10.1.1 Your System Environment 217
10.1.2 Goals and Objectives 218
10.1.3 Reviewing Your Policy 218
10.1.4 Requirements and Constraints 219
10.2 Making Sense of Products 220
10.2.1 Understanding the Problem Space 220
10.2.2 Is the Product Scalable? 221
10.2.3 How Did You Test This? 221
10.2.4 Is This Product a Tool or Is It an Application? 222
10.2.5 Buzzwords versus Wisdom 223
10.2.6 Anticipated Life of Product 224
10.2.7 Training Support 224
10.2.8 Prioritized Goals of Product 224
10.2.9 Product Differentiation 225
10.3 Mapping Policy to Configurations 225
10.3.1 Converting Policy to Rules 225
10.3.2 Subject-Objects to Real World 226
10.3.3 Monitoring Policy versus Security Policy 227
10.3.4 Testing Assertions 227
10.4 Show Time! Incident Handling and Investigation 227
10.4.1 Scout's Honor 228
10.4.2 Best Practices 228
10.4.3 When the Balloon Goes Up 229
10.4.4 Dealing with Law Enforcement 230
10.4.5 Expectations 231
10.4.6 Damage Control 231
10.4.7 Dealing with Witch Hunts 232
10.5 Conclusion 232
Endnotes 233

For Strategists 235
11.1 Building a Case for Security 235
11.1.1 Assembling Information 236
11.1.2 What Is the Organization Trying to Accomplish? 236
11.1.3 How Does Security Fit Into Overall Business Goals? 236
11.1.4 Where Does Information Security Fit Into the Corporate Risk-Management Program? 237
11.1.5 What Do We Need to Secure the System? 238
11.1.6 Finding Allies 239
11.1.7 Overcoming Management Resistance 241
11.2 Defining Requirements for IDS 242
11.2.1 Revisiting Goals and Objectives 242
11.2.2 What Are the Threats? 242
11.2.3 What Are Our Limitations? 243
11.2.4 Considerations in Adopting Intrusion Detection and System Monitoring 243
11.3 Marketing Hype versus Real Solutions 244
11.3.1 What Product Is Best Fitted to Us and Our Goals? 244
11.3.2 How Painful Is This Product to Install? 245
11.3.3 How Painful Is This Product to Run? 245
11.3.4 What Are the Expectations of the Personnel? 246
11.3.5 Who Was the Dream Customer for Whom This Product Was Designed? 246
11.4 Integrating Security Into a Legacy Environment 246
11.4.1 Assessing the Existing Systems 247
11.4.2 Leveraging Investments in Security 247
11.4.3 Dealing with "Wetware"—the Humans in the System 248
11.4.4 Handling Conflicts 249
11.5 Dealing with the Effects of Corporate Transitions 250
11.5.1 Mergers and Acquisitions 250
11.5.2 Strategic Partners 250
11.5.3 Globalization 251
11.5.4 Expansion and Contraction 251
11.5.5 Going from Private to Public 252
11.6 Conclusion 252
Endnotes 253

For Designers 255
12.1 Requirements 256
12.1.1 Good versus Great Intrusion Detection 256
12.1.2 Different Approaches to Security 258
12.1.3 Policies—One Size Does Not Fit All 260
12.2 Security Design Principles 262
12.2.1 Economy of Mechanism 262
12.2.2 Fail-Safe Defaults 263
12.2.3 Complete Mediation 263
12.2.4 Open Design 263
12.2.5 Separation of Privilege 264
12.2.6 Least Privilege 264
12.2.7 Least Common Mechanism 265
12.2.8 Psychological Acceptability 265
12.3 Surviving the Design Process 265
12.3.1 Establishing Priorities 265
12.3.2 On Threat Curmudgeons 266
12.3.3 Striking and Maintaining Balance 267
12.4 Painting the Bull's Eye 268
12.4.1 Gauging Success 268
12.4.2 False Starts 269
12.4.3 Testing Approaches 269
12.4.4 Measuring Network-Based Performance 270
12.5 Advice from the Trenches 271
12.5.1 Use Good Engineering Practices 271
12.5.2 Secure Sensors 272
12.5.3 Pay Attention to Correct Reassembly 272
12.5.4 Don't Underestimate Hardware Needs 272
12.5.5 Don't Expect Trusted Sources of Attack Data 272
12.5.6 Think Through Countermeasures 273
12.5.7 No Support for Forensics 273
12.5.8 Support Modern Security Features 273
12.6 Conclusion 273
Endnotes 274
Future Needs 275
13.1 Future Trends in Society 276
13.1.1 Global Villages and Marketplaces 276
13.1.2 Privacy as an Economic Driver 276
13.1.3 A Different Kind of War 277

13.1.4 Sovereignty 277

13.2 Future Trends in Technology 277

13.2.1 Changes in the Network Fabric 277

13.2.2 Open Source Software 278

13.2.3 Advances in Wireless Networking 278

13.2.4 Ubiquitous Computing 279

13.3 Future Trends in Security 279

13.3.1 Management 279

13.3.2 Privacy-Sparing Security 281

13.3.3 Information Quality versus Access Control 282

13.3.4 Crypto, Crypto Everywhere . . . 282

13.3.5 The Erosion of Perimeters 282

13.3.6 Liability Transfer versus Trust Management 283

13.4 A Vision for Intrusion Detection 283

13.4.1 Capabilities 283

13.4.2 Highly Distributed Architectures 284

13.4.3 911 for Security Management 285

13.4.4 Ubiquitous Information Sources 285

13.4.5 Silicon Guards 285

13.4.6 Emphasis on Service, Not Product 286

13.5 Conclusion 286

Endnotes 287

Appendix A Glossary 289

Appendix B Bibliography 297

Appendix C Resources 315

Books 315

Intrusion Detection and Associated Technologies 315

Security References and Textbooks 315

Information Warfare, Critical Systems, and National Policy 316

Introduction to Computer and Network Security 316

Cryptography 316

Firewalls 316

War Stories 317

Specific Application Venues 317

Cybercrime and Law Enforcement 317

For Fun 317

WWW Resources 317
Security Portals 318
Vulnerability Information Sources 318
Organizations 318
Government Sites 319
Academic Sites 319
Commercial Products, Services, and Research 319
Miscellaneous Intrusion Detection References 320

Appendix D Checklist 321

Index 323

CHAPTER 1

The History of Intrusion Detection

"Life was simple before World War II. After that, we had systems."
- Admiral Grace Hopper

When I explain intrusion detection to those not familiar with network security, it's usually easy to describe what intrusion detection systems do: "It's a burglar alarm for computers and networks," or "It looks for criminals breaking into a computer system and lets someone know about it." Most people understand that when systems handle things that are considered valuable, the systems themselves are natural targets of attack.

Although the goals of intrusion detection systems may be intuitively obvious to both technical and nontechnical users, many people are not aware of the history of intrusion detection research and development. This lack of information results in repeating mistakes made in the past or needlessly settling for suboptimal approaches to critical functions.

Intrusion detection has merged traditional electronic data processing (EDP) and security audit with optimized pattern-matching and statistical techniques. Intrusion detection has become an integral part of modern network security technology. In this section, I describe the history of audit and intrusion detection from the perspective of the people who did the initial research and development and their projects.

1.1 Audit: Setting the Stage for Intrusion Detection

Before intrusion detection, there was audit. *Audit* is defined as the process of generating, recording, and reviewing a chronological record of system events. People audit systems to accomplish a variety of goals. These goals include the following:

- To assign and maintain personal accountability for system activities
- To reconstruct events
- To assess damage

1.1.4 Audit and Military Models of Computer Security

The U.S. Department of Defense (DOD) backed an extensive research effort during the 1970s, which explored security policies, guidelines, and controls for operating "trusted systems," culminating in the DOD Security Initiative of 1977.

Trusted systems were defined as "systems that employ sufficient hardware and software assurance measures to allow their use for simultaneous processing of a range of sensitive or classified information."[3] Thus, trusted systems were designed from the ground up in a way that allowed military and intelligence organizations to place information of different sensitivity levels (typically corresponding to levels of classification) on the same computer system. The Trusted Systems Initiative provided a venue in which the computer security experts of the era explored the features and protections that were necessary for trusted systems to function. (Trusted systems are discussed in more depth in Chapter 3.)

During the initial explorations, researchers debated whether security audit mechanisms would contribute to the assurance level of a trusted system. Ultimately, the audit mechanism was indeed included as part of the *Trusted Computer System Evaluation Criteria*[4] ("Orange Book") requirements for systems evaluated at trust levels C2 and above. The series of documents that outlined the DOD's Trusted Systems Initiative are often referred to as the "Rainbow series," in a reference to the brightly colored covers of the documents.

A document, which addresses the issue of audit in trusted systems, is included in the Rainbow series. It is the "Tan Book," titled *A Guide to Understanding Audit in Trusted Systems.*

The Tan Book outlines five security goals for audit mechanisms:

- To allow the review of patterns of access (on a per-object and per-user basis) and the use of protection mechanisms of the system
- To allow the discovery of both insider and outsider attempts to bypass protection mechanisms
- To allow the discovery of a transition of a user from a lesser to a greater privilege level; for example, when a user moves from clerical to system administrator roles
- To serve as a deterrent to users' attempts to bypass system-protection mechanisms
- To serve as yet another form of user assurance that attempts to bypass the protection will be recorded and discovered, with sufficient information recorded to allow damage control

Although the Tan Book (as well as much of the Rainbow series) reflects a rather centralized mainframe view of computing, its principles of security audit still apply.[5]

Note

MIDAS, one of the first intrusion detection systems that monitored an operational system connected to the Internet, gave a fascinating view of the Internet threat. Dockmaster was an attractive target for attack due to its affiliation with the Defense Department. Perhaps the most interesting insight that MIDAS gave us was a demonstration of the value of strong identification and authentication (I&A) mechanisms. In the late 1980s, after MIDAS came online, the NCSC decided to utilize token-based I&A as a replacement for weaker password mechanisms. In the scheme selected, users had a calculator-style token, protected by a PIN. When someone logged into Dockmaster, the system issued a multidigit challenge; this challenge was entered into the token, and the resulting multidigit response was sent back to Dockmaster, at which time the user session began.

MIDAS allowed the Dockmaster security staff to see the effects of enacting this stronger login mechanism. Doorknob-rattling and password-guessing incidents dropped dramatically after the token-based I&A system was in place. This effect emphasizes again the importance of thinking holistically when determining a protection strategy for systems.

The intrusion detection system could have continued to record attempts to hack into the system by password-guessing or other such attacks on weaker I&A mechanisms. Attackers might have been deterred, but only after a great deal of time and energy were spent on investigating the incident—tracking down the attacker, going through the phases of a criminal investigation and prosecution, and hoping for a sufficiently harsh sentence to discourage further attacks. The desired effect (to make external attackers stop) was much more quickly and easily accomplished by using a strong protection mechanism at the system access point.

Another even more important point is that, despite strengthening I&A to a point where external attackers were thwarted, the organization continued to run MIDAS to monitor for insider abuse.

1.2.3.5 NADIR

Network Audit Director and Intrusion Reporter[14] (NADIR) was developed by the Computing Division of Los Alamos National Laboratory to monitor user activities on the Integrated Computing Network (ICN) at Los Alamos. This network is Los Alamos's main computer network and serves more than 9,000 users—connecting supercomputers, local and remote terminals, workstations, network services machines, and data communications interfaces. NADIR monitors the network by processing audit trails generated by specialized network service nodes. It was designed to run on Sun UNIX workstations and, like many other systems of the time, it performs a combination of expert rule-based analysis and statistical profiling. NADIR is written in SQL an

runs on a Sybase database management system, using some of Sybase's internal triggers and other features.

NADIR remains one of the most successful and durable intrusion detection systems of the 1980s and has been extended to monitor systems beyond the ICN at Los Alamos. NADIR continues to monitor the ICN at the time of this publication, and the team continues to modify the system to accommodate new threats and target systems. The principal architect for NADIR is Kathleen Jackson.

1.2.3.6 NSM

The Network System Monitor (NSM) was developed at the University of California at Davis to run on a Sun UNIX workstation. It represented the first foray into monitoring network traffic and using that traffic as the primary data source. Before this time, most intrusion detection systems consumed information from operating system audit trails or keystroke monitors. The general architecture of the NSM is still reflected in many commercial intrusion detection products at the time of this publication. The NSM functioned by doing the following:

- Placing the system's Ethernet network interface card into promiscuous mode (in which each network frame generates an interrupt, thereby allowing the monitoring system to listen to all traffic, not just those packets addressed to the system)
- Capturing network packets
- Parsing the protocol to allow extraction of pertinent features as shown in Figure 1.4
- Using a matrix-based approach to archive and analyze the features, both for statistical variances from normal behavior and for violations of pre-established rules

NSM was a significant milestone in intrusion detection research because it was the first attempt to extend intrusion detection to heterogeneous network environments. It was also one of the first intrusion detection systems to run on an operational system (the computer science department local area network at UC Davis). In a widely cited, two-month test of NSM, it monitored more than 111,000 connections on the network segment, correctly identifying more than 300 of them as intrusions. The system administrators for the network discovered less than one percent of these intrusions. This test emphasized the need for and the effectiveness of intrusion detection systems as part of the protection suite. Principal architects for NSM were Karl Levitt, Todd Heberlein, and Biswanath Mukherjee of the University of California at Davis.[15]

An additional human input comes in the form of user interaction with intrusion detection control components. This type of input can consist of system configuration or policy entry at the time of system installation and setup. It can also take the form of active interaction with the system console, responding to detected problems by directing the system to take additional action. Several generations of intrusion detection systems are likely to be required before detection schemes are mature and reliable enough to allow unsupervised operation. For some environments, the total automation of intrusion detection analysis functions may never be appropriate. In the meantime, you should consider intrusion detection systems as diagnostic tools that allow you to "see" system activity through a security-savvy prism, using this higher-level view to gain additional expertise in recognizing and dealing with security problems.

3.4 *Information from Other Security Products*

In general, the more event information that is considered in performing intrusion detection analysis, the more accurate and sensitive the results. This relationship is especially true in performing intrusion detection on networks, where stand-alone security products are common.

Many firewalls, I&A systems, access control systems, and other security devices and subsystems generate their own activity logs. These logs contain information that is, by definition, of security significance; they are therefore of particular value to the intrusion detection process. Including these logs as information sources is an obvious way to improve the quality of the intrusion detection process.

The process of integrating and analyzing event logs from other components of the system security infrastructure represents a significant and enduring role that intrusion detection systems can play. This role continues to be relevant, even as strong encryption or other measures address those threats we consider of greatest concern today. Although technical environments change, the attack strategies of adversaries remain relatively stable. Because an elementary step in attacking a system is to locate, investigate, and then nullify the existing system protections, monitoring security products will remain a stable requirement.

3.4.1 *An Example of a Security Product Data Source*

Table 3.4 presents a format diagram of the firewall log file generated by Firewall-1, a CheckPoint Technologies product. It allows you to see the transactions processed by the firewall, including mappings of ostensible sources and destinations of connections, the names of system objects associated with the transactions, and other information that was selected for inclusion.